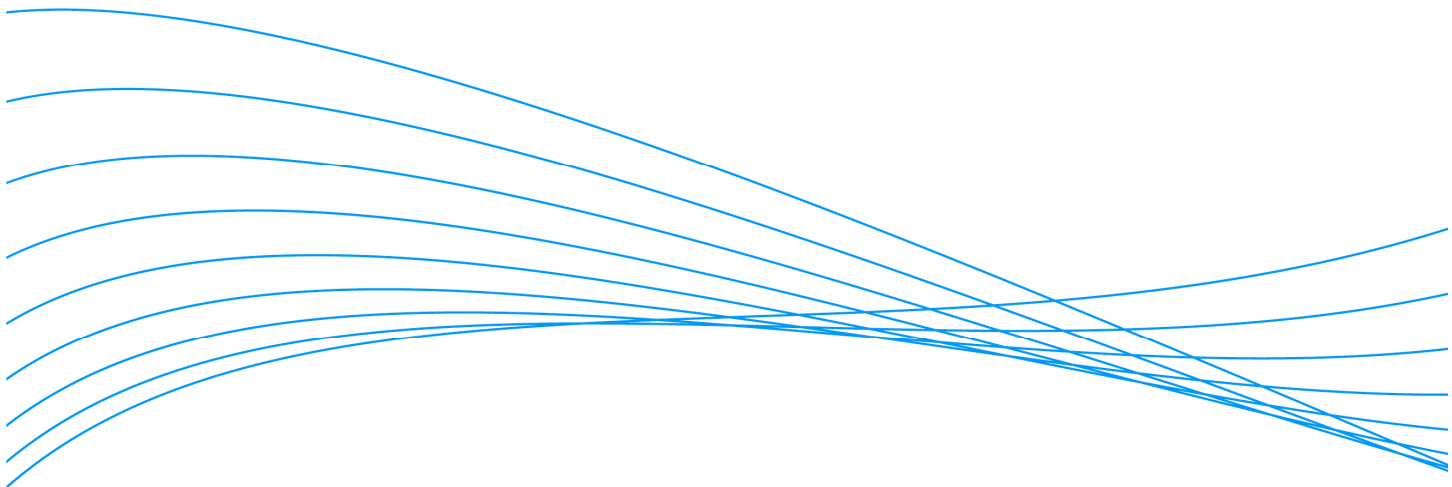


Protecting the Extended Enterprise Network

Security Strategies and Solutions from ProCurve Networking



Introduction	2
Today's Network Security Landscape.....	2
Accessibility	2
User Types.....	3
Mobility	3
Convergence	3
Enacting a Sound Security Strategy	4
ProCurve Networking Adaptive EDGE Architecture™	4
ProCurve Security Framework	5
Infrastructure	6
Access.....	6
Availability	6
Privacy	6
ProCurve Network Security Products and Solutions.....	7
Summary.....	8
For more information.....	9

Introduction

As network security has risen in awareness and priority, so too have the matters that complicate it. No longer simply a 'check box' item, network security has become a chief concern for enterprises and the focus has expanded from just the Internet connection to the local area network (LAN), wireless LAN (WLAN) and wide area network (WAN).

According to Gartner, defending the enterprise network "in depth" is vital to protecting an organization. However, doing so at the expense of security at the perimeter is not a sound strategy. Therefore, securing the network perimeter is more important than ever¹.

It is no longer adequate to have exclusively centralized, host-based security with Internet firewalls and intrusion detection. Today's enterprises need a security strategy that includes detection and enforcement at every point of network access, for all user types. This means providing intelligent access services at the edge of the network, where users connect – whether it is via a switch in a wiring closet or a wireless access point. Network and policy management, however, must remain centrally managed for crucial control.

This paper provides an overview of the infrastructure security issues executives and IT managers face as enterprise networks become more public, more converged and more mobile. It also outlines new security strategies, the ProCurve Security Framework and the advantages of providing secure access control at the network edge.

Today's Network Security Landscape

Security used to mean setting up a firewall as a perimeter line of defense to keep trusted users on the inside and distrusted users on the outside. However, in today's world of remote workers, wireless users, trading partners, customers and hackers, the idea of an infrastructure's perimeter is being redefined. There is no longer a singular gate that facilitates access to an enterprise network.

Several key business and technology developments – including network accessibility, user types, mobility and convergence – are blurring the notion of a network's edge, increasing infrastructure vulnerabilities and complicating the ways in which to secure them.

Accessibility

Access control is a crucial security concern as it is now common to have pervasive, live ports nearly everywhere within an enterprise campus. Where organizations once had a direct and static correspondence between an access port, a PC and a user, modern LANs, WLANs and WANs extend far beyond the marginally controlled office environment.

Today there are innumerable methods to access enterprise network applications and resources, including wired clients that access the network via switches and routers, wireless clients that connect to Wi-Fi access points, dial-up clients using the Internet and virtual private network (VPN) software or remote access services (RAS).

Furthermore, enterprises are learning that providing network connectivity and facilitating access to specific information and resources are two entirely separate notions, and authorized access is only the tip of the iceberg in terms of network security. Organizations need to control not only who gets onto the network, but also what resources each user is able to access as well as where and when those resources can be accessed. Without the proper safeguards in place, infiltrating enterprise network applications and resources can be easy for unauthorized users.

¹ "Securing the Network Perimeter is More Important Than Ever." Gartner. March 23, 2005. Article.

User Types

The management of user types becomes increasingly complex as the enterprise network environment expands and changes to include full, part-time and temporary employees, contract workers, remote workers, guests, partners, resellers and customers. Each user type requires different access abilities and network resources (see Figure 1).

Where a network manager used to be concerned only with external threats, today's network manager must also be concerned with internal problems, both real and potential. Unfortunately, it is no longer a given that anyone with authorized network access is completely trustworthy. Companies must implement network-based security with zones for different users combined with the conventional host-based security and Internet firewalls.

Mobility

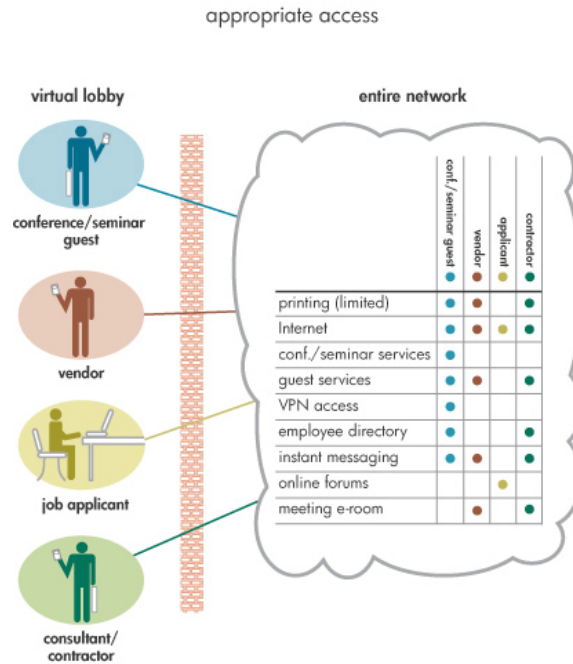
The network is extending its reach to provide mobile connectivity with local wireless technology, public high-bandwidth wireless hotspots and digital cellular to address the needs of anytime, anywhere communications. Wireless networks and devices make the security challenge obvious. WLAN technology and use are rapidly evolving and growing, rogue access points litter corporate enterprises and the range of potentially mobile and always mobile digital appliances continues to diversify and proliferate.

The emergence of these mobile network access devices, next-generation convergence solutions and inexpensive wireless access points, combined with open ports existing in many campus public areas, provides endless connectivity opportunities and security vulnerabilities.

Convergence

As voice, video and data convergence is introduced to the network, new policies and procedures must be put in place. Core network security applications that performed well scanning and policing data transactions may now cause problems for voice and video applications sensitive to latency and jitter. This raises an entirely new set of security issues in conjunction with providing quality-of-service (QoS) for next-generation applications.

Figure 1. Controlling Access to the Network and Its Resources.



Enacting a Sound Security Strategy

Ensuring an enterprise's network and data assets are fully protected extends beyond specific security products and features. It requires a sound, holistic security strategy that addresses three key business issues.

First, an organization needs an affordable, integrated, secure enterprise network that spans all locations. The network must offer simplified, secure, remote access via an integrated, versatile and affordable platform for interconnecting multiple sites and remote users.

Second, the organization needs a network that is resilient and available even when under attack. As such, the infrastructure must defend against unknown worms and other malicious agents to prevent network downtime and avoid costly lost productivity and business function breakdowns. It also must be able to withstand unintentional problems that can have the same devastating effects as malicious agents, such as improper configuration or faulty equipment.

Third, as a business mobilizes, so must its network security. The infrastructure must provide a secure wireless extension to the wired network that is easy to deploy and manage, well integrated and fully transparent to mobile users.

ProCurve Networking Adaptive EDGE Architecture™

ProCurve has developed an innovative approach to network design, embodied in the ProCurve Networking Adaptive EDGE Architecture™. Unlike traditional network designs, it extends intelligence beyond core devices to the network edge and delivers a new, unified approach to secure, mobile, multi-service networks. The Adaptive EDGE Architecture is built on two key principles: the need to maintain complete command of

the network in a centralized manner and push control to the network edge where users connect.

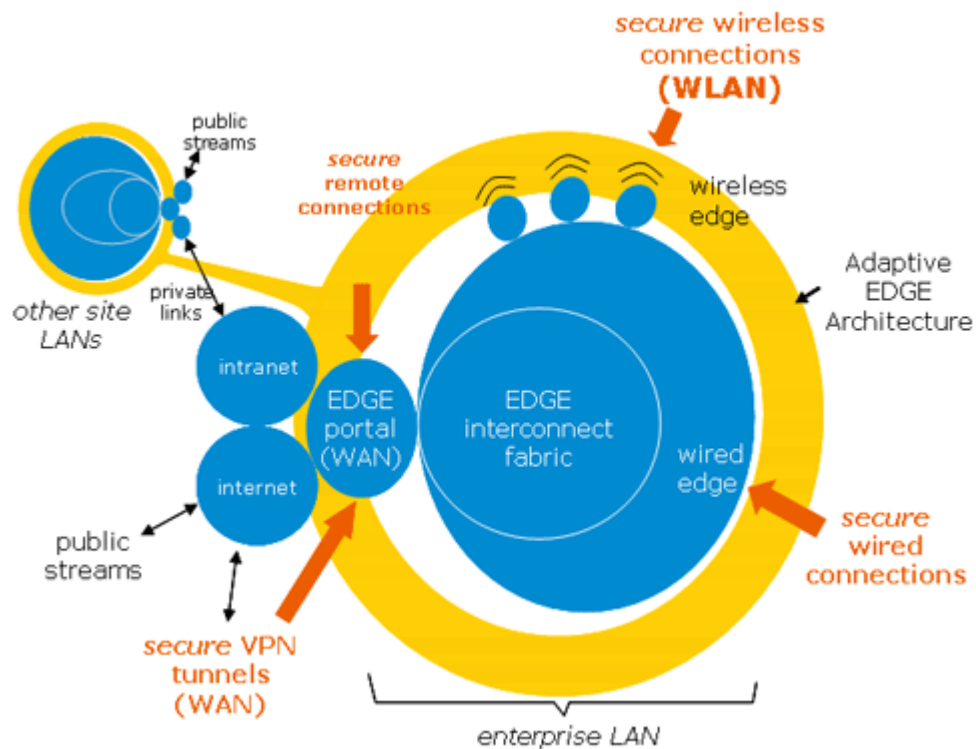
Command from the center provides controlled access to critical network components based on an individual user's business needs. This approach shelters secure data and applications not needed by that user, protecting an organization's digital assets. The network edge is where security policies must be enforced, where the user connects after being authenticated at a central command resource. Without control to the edge, decisions about security and traffic must be deferred to the network core, opening the network to security attacks after access is physically attained yet before authorization is granted.

With potential threats to security coming from any number of directions, it is essential that network access be easily controlled from the center but enforced at the edge, where it can most effectively protect network assets.

ProCurve Security Framework

Based on the Adaptive EDGE Architecture, ProCurve offers a comprehensive security framework that is able to control which users access which resources depending on the needs of their job (see Figure 2).

Figure 2. ProCurve Security Framework.



ProCurve's unified approach addresses both wired and wireless access and secures all end-user connection methods to the enterprise LAN, WLAN and WAN. The ProCurve Security Framework meets the three key business requirements listed above, and delivers utmost protection in the areas of Infrastructure, Access, Availability and Privacy.

Infrastructure

Infrastructure elements are the secure physical foundation of switches, access points and WAN devices. ProCurve solutions are able to authenticate infrastructure devices, provide secure management communications, protect infrastructure devices from attack and offer resiliency against unanticipated faults.

Access

Access features facilitate a personalized network experience based on the user and the device through which they are connecting. ProCurve security solutions are able to authenticate users, hosts, servers and services, ensure host integrity and enforce access rights.

An emerging aspect of access security and control is Identity Driven Management, which represents a new way of administering the network. ProCurve offers Identity Driven Management functionality that dynamically configures the network so it behaves differently for each user. With Identity Driven Management, ports and points of access configure themselves according to each user, their access rights, the device through which they are seeking access and the applications they are authorized to utilize.

Availability

Availability features must be able to detect and contain security breaches and other malfunctions. ProCurve security solutions offer several availability features, including anomaly detection, intrusion detection/protection and new, innovative virus throttling functionality.

Privacy

Privacy features help protect user data being stored on or moved throughout the network. ProCurve solutions preserve the integrity of data and ensure private communication by using the latest encryption technologies.

Figure 3. ProCurve Security Framework Capabilities.

	Infrastructure	Access	Availability (network immunity)	Privacy
Definition	Secure physical foundation of switches, access points & WAN devices	Personalized network experience based on user & device type	Security breach detection and containment	Non-reputable private communication
Key Elements	<ul style="list-style-type: none"> • Authenticate infrastructure devices • Secure mgmt communications • Protect infrastructure devices from attack 	<ul style="list-style-type: none"> • Authenticate users, hosts, servers and services • Ensure host integrity • Enforce access rights 	<ul style="list-style-type: none"> • Virus throttling • Anomaly detection • Intrusion detection and protection 	<ul style="list-style-type: none"> • Protect user data across the network
ProCurve Solutions Focus	<ul style="list-style-type: none"> • Trusted infrastructure • Secure management 	<ul style="list-style-type: none"> • User authentication • Device authentication • Traffic policy enforcement 	<ul style="list-style-type: none"> • Resiliency • Anomaly detection • Auxiliary services 	<ul style="list-style-type: none"> • Point-to-point • End-to-end

With a distinct focus on the four pillars of Infrastructure, Access, Availability and Privacy, the ProCurve Security Framework delivers:

- A secure, resilient network that is able to withstand a variety of malfunctions and malicious agents and be available even when under attack.
- Security features integrated into the fabric of the network so that users receive the same experience and the network receives the same protection whether traffic is wired or wireless, local or remote.
- Affordability, versatility and ease-of-management.

ProCurve Network Security Products and Solutions

Robust security capabilities and features – embedded in ProCurve switches, wireless products and routers – are available today to fully secure enterprise networks.

For infrastructure security, all managed ProCurve products utilize industry standards and encryption technologies as well as physical access security features, such as disable reset switches, for controlling network access and securing traffic. These capabilities are easily administered with ProCurve Manager Plus network management software.

For access control, ProCurve offers a comprehensive Access Control Security solution (ACS) and Identity Driven Manager (IDM) that provide authentication, ensure host integrity and enforce access rights. ACS provides basic authentication via 802.1x, Web or MAC based approaches in conjunction with RADIUS servers. IDM dynamically applies security, access and performance settings to network infrastructure devices based on approved users, location and time via centralized policy management. A plug-in for ProCurve Manager Plus, IDM is ideal for medium to large organizations requiring access

control due to high user turnover or a need to adapt the network for specific user profiles and access rights.

To keep a network up and running even when a virus is threatening to disrupt business operations, new technologies like virus throttling in the ProCurve 5300 intelligent edge switch stop the spread of viruses in their tracks. The most common method of protecting wired and wireless networks is to implement anti-virus software on each individual client. These solutions utilize signature recognition to identify the physical characteristics of a documented virus and, once recognized, prevent it from entering the network. Unfortunately, these tools are fundamentally reactive and only effective when dealing with *known* viruses. They are not able to recognize or stop new threats that sprout daily.

Connection-rate filtering based on virus throttling technology is a new, ProCurve-developed solution that addresses these concerns. Virus throttling is unique in that it identifies the behavioral characteristics of a network under attack (i.e. the number of connections a computer is attempting to make per second) instead of the physical characteristics of a known virus (i.e. program code). In doing so, it is able to automatically discover attacks by previously unknown threats and hamper them by immediately restricting bandwidth, giving network managers the time necessary to implement a response.

Summary

It is inevitable. Security will remain a vital component for the viability of information systems. Network security is and will continue to be critical as real-time communication needs increase, the workforce becomes more mobile and enterprises implement multi-service networks.

Establishing effective network security requires solutions that adapt to new and existing vulnerabilities, minimize risks and protect information assets at any cost. ProCurve security solutions move important access decisions to the edge of the network where users and applications connect. Core resources are freed to provide the high bandwidth interconnect functions for which they are meant, meaning enterprise networks are optimized to perform better. Furthermore, effective control to the edge helps enable the support necessary for network convergence and a mobile workforce.

With several layers of built-in security that take advantage of the latest standards-based security features to protect data, ProCurve's diverse array of security products and services bring trust, reliability and flexibility to enterprise networking.

For more information

To learn more about ProCurve solutions, contact your local ProCurve sales representative or visit the company's Web site at <http://www.procurve.com>.

For a list of ProCurve Elite Partners that can provide ProCurve security solutions, go to <http://www.procurve.com>.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA0-0366ENW, 4/2005